

CLAIMS

- 1 1. An apparatus comprising:
2 at least one processor;
3 a memory coupled to the at least one processor;
4 a first program residing in the memory;
5 a second program residing in the memory;
6 a dynamic key generation mechanism that dynamically generates public/private
7 key pairs; and
8 an inter-program authentication mechanism that authenticates the first program to
9 the second program using a public/private key pair that is dynamically generated by the
10 dynamic key generation mechanism.
- 1 2. The apparatus of claim 1 wherein the first program includes an authentication
2 mechanism that authenticates a user.
- 1 3. The apparatus of claim 1 wherein, after the inter-program authentication
2 mechanism authenticates the first program to the second program, the second program
3 performs identity mapping from an identity asserted by the first program to an identity
4 understood by the second program.
- 1 4. The apparatus of claim 1 wherein the first program authenticates to the second
2 program using a first authentication token that is digitally signed by the first program
3 using a private key that is dynamically generated by the dynamic key generation
4 mechanism.

1 5. The apparatus of claim 4 wherein the first authentication token comprises:
2 information about a user that authenticates with the first program;
3 information about the first program;
4 information about the second program; and
5 a digital signature of the first program using a private key for the first program
6 generated by the dynamic key generation mechanism.

1 6. The apparatus of claim 4 wherein the second program verifies the first
2 authentication token by querying a public key authority for the public key corresponding
3 to the first program.

1 7. The apparatus of claim 6 wherein the second program verifies the first
2 authentication token by verifying the digital signature of the first program using the
3 public key for the first program retrieved from the public key authority.

1 8. The apparatus of claim 4 wherein the second program authenticates to the first
2 program, if required, by digitally signing the first authentication token using a private key
3 corresponding to the second program to generate therefrom a second authentication token,
4 and returning the second authentication token to the first program.

1 9. The apparatus of claim 8 further comprising a third program residing in the
2 memory, wherein the second program authenticates to the third program by generating a
3 third authentication token from the first authentication token received from the first
4 program, and sending the third authentication token to the third program.

1 10. The apparatus of claim 9 wherein the third program verifies the third
2 authentication token by querying a public key authority for the public key corresponding
3 to the second program.

1 11. The apparatus of claim 1 further comprising log file that is written to each time a
2 program verifies an authentication token.

1 12. An apparatus comprising:
2 at least one processor;
3 a memory coupled to the at least one processor;
4 a first program residing in the memory, the first program including an
5 authentication mechanism that authenticates a user;
6 a second program residing in the memory;
7 a dynamic key generation mechanism that dynamically generates public/private
8 key pairs;
9 a public key authority that publishes public keys generated by the dynamic key
10 generation mechanism; and
11 an inter-program authentication mechanism that authenticates the first program to
12 the second program using a first authentication token that is digitally signed by the first
13 program using a private key that is dynamically generated by the dynamic key generation
14 mechanism.

1 13. The apparatus of claim 12 wherein, after the inter-program authentication
2 mechanism authenticates the first program to the second program, the second program
3 performs identity mapping from an identity asserted by the first program to an identity
4 understood by the second program.

1 14. The apparatus of claim 12 wherein the first authentication token comprises:
2 information about a user that authenticates with the first program;
3 information about the first program;
4 information about the second program; and
5 a digital signature of the first program using a private key for the first program
6 generated by the dynamic key generation mechanism.

1 15. The apparatus of claim 12 wherein the second program verifies the first
2 authentication token by querying the public key authority for the public key
3 corresponding to the first program.

1 16. The apparatus of claim 15 wherein the second program verifies the first
2 authentication token by verifying the digital signature of the first program using the
3 public key for the first program retrieved from the public key authority.

1 17. The apparatus of claim 12 wherein the second program authenticates to the first
2 program, if required, by digitally signing the first authentication token using a private key
3 corresponding to the second program to generate therefrom a second authentication token,
4 and returning the second authentication token to the first program.

1 18. The apparatus of claim 17 further comprising a third program residing in the
2 memory, wherein the second program authenticates to the third program by generating a
3 third authentication token from the first authentication token received from the first
4 program, and sending the third authentication token to the third program.

1 19. The apparatus of claim 18 wherein the third program verifies the third
2 authentication token by querying the public key authority for the public key
3 corresponding to the second program.

1 20. The apparatus of claim 12 further comprising a log file that is written to each time
2 a program verifies an authentication token.

1 21. An apparatus comprising:
2 at least one processor;
3 a memory coupled to the at least one processor;
4 a first program residing in the memory;
5 a second program residing in the memory;
6 a third program residing in the memory;
7 a dynamic key generation mechanism that dynamically generates public/private
8 key pairs; and
9 an inter-program authentication mechanism that authenticates the first program to
10 the second program using a first authentication token generated by the first program using
11 a public/private key pair corresponding to the first program, and that authenticates the
12 second program to the third program using a second authentication token that includes all
13 information in the first authentication token.

- 1 22. A method for a first program to authenticate to a second program, the method
2 comprising the steps of:
- 3 (A) dynamically generating a public/private key pair for the first program;
4 (B) the first program generating a first authentication token using the private key
5 dynamically generated in step (A); and
6 (C) the second program verifying the first authentication token using the public
7 key dynamically generated in step (A).
- 1 23. The method of claim 22 wherein the second program verifies the first
2 authentication token in step (C) by verifying a digital signature of the first program in the
3 authentication token using the public key for the first program.
- 1 24. The method of claim 22 further comprising the step of authenticating a user to the
2 first program.
- 1 25. The method of claim 22 further comprising the step of performing identity
2 mapping from an identity asserted by the first program to an identity understood by the
3 second program.
- 1 26. The method of claim 22 wherein the first authentication token comprises:
2 information about a user that authenticates with the first program;
3 information about the first program;
4 information about the second program; and
5 a digital signature of the first program using a private key for the first program
6 generated by the dynamic key generation mechanism.

1 27. The method of claim 22 further comprising the steps of:
2 (D) dynamically generating a public/private key pair for the second program;
3 (E) the second program digitally signing the first authentication token using the
4 private key generated in step (D) to generate therefrom a second authentication token; and
5 (F) returning the second authentication token to the first program to authenticate
6 the second program to the first program.

1 28. The method of claim 22 further comprising the step of the second program
2 authenticating to a third program by generating a third authentication token from the first
3 authentication token and sending the third authentication token to the third program.

1 29. The method of claim 28 further comprising the step of the third program verifying
2 the third authentication token by using the public key generated in step (D).

1 30. The method of claim 22 further comprising the step of writing to a log file that is
2 written to each time a program verifies an authentication token.

1 31. A method for a first program to authenticate to a second program, the method
2 comprising the steps of:
3 (A) dynamically generating a public/private key pair for the first program;
4 (B) sending the public key for the first program to a public key authority;
5 (C) dynamically generating a public/private key pair for the second program;
6 (D) sending the public key for the second program to the public key authority;
7 (E) the first program generating a first authentication token using the private key
8 for the first program; and
9 (F) the second program verifying the first authentication token by querying the
10 public key authority for the public key corresponding to the first program.

1 32. The method of claim 31 wherein the second program verifies the first
2 authentication token in step (F) by verifying a digital signature of the first program in the
3 authentication token using the public key for the first program retrieved from the public
4 key authority.

1 33. The method of claim 31 further comprising the step of authenticating a user to the
2 first program.

1 34. The method of claim 31 further comprising the step of performing identity
2 mapping from an identity asserted by the first program to an identity understood by the
3 second program.

1 35. The method of claim 31 wherein the first authentication token comprises:
2 information about a user that authenticates with the first program;
3 information about the first program;
4 information about the second program; and
5 a digital signature of the first program using a private key for the first program
6 generated by the dynamic key generation mechanism.

1 36. The method of claim 31 further comprising the steps of:
2 (G) dynamically generating a public/private key pair for the second program;
3 (H) the second program digitally signing the first authentication token using the
4 private key generated in step (G) to generate therefrom a second authentication token; and
5 (I) returning the second authentication token to the first program to authenticate
6 the second program to the first program.

1 37. The method of claim 31 further comprising the step of the second program
2 authenticating to a third program by generating a third authentication token from the first
3 authentication token and sending the third authentication token to the third program.

1 38. The method of claim 37 further comprising the step of the third program verifying
2 the third authentication token by using the public key corresponding to the second
3 program.

1 39. The method of claim 31 further comprising the step of writing to a log file that is
2 written to each time a program verifies an authentication token.

1 40. A method for authenticating a first program to a third program, the method
2 comprising the steps of:
3 authenticating the first program to a second program using a first authentication
4 token generated by the first program using a public/private key pair corresponding to the
5 first program; and
6 authenticating the second program to the third program using a second
7 authentication token that includes all information in the first authentication token.

1 41. A program product comprising:
2 (A) an inter-program authentication mechanism that authenticates a first program
3 to a second program using a public/private key pair that is dynamically generated by a
4 dynamic key generation mechanism; and
5 (B) computer-readable signal bearing media bearing the inter-program
6 authentication mechanism.

1 42. The program product of claim 41 wherein the computer-readable signal bearing
2 media comprises recordable media.

1 43. The program product of claim 41 wherein the computer-readable signal bearing
2 media comprises transmission media.

1 44. The program product of claim 41 wherein the first program includes an
2 authentication mechanism that authenticates a user.

1 45. The program product of claim 41 wherein, after the inter-program authentication
2 mechanism authenticates the first program to the second program, the second program
3 performs identity mapping from an identity asserted by the first program to an identity
4 understood by the second program.

1 46. The program product of claim 41 wherein the first program authenticates to the
2 second program using a first authentication token that is digitally signed by the first
3 program using a key that is dynamically generated by the dynamic key generation
4 mechanism.

1 47. The program product of claim 46 wherein the first authentication token
2 comprises:
3 information about a user that authenticates with the first program;
4 information about the first program;
5 information about the second program; and
6 a digital signature of the first program using a private key for the first program
7 generated by the dynamic key generation mechanism.

1 48. The program product of claim 46 wherein the second program verifies the first
2 authentication token by querying the public key authority for the public key
3 corresponding to the first program.

1 49. The program product of claim 48 wherein the second program verifies the first
2 authentication token by verifying the digital signature of the first program using the
3 public key for the first program retrieved from the public key authority.

1 50. The program product of claim 46 wherein the second program authenticates to the
2 first program, if required, by digitally signing the first authentication token using a private
3 key corresponding to the second program to generate therefrom a second authentication
4 token, and returning the second authentication token to the first program.

1 51. The program product of claim 50 further comprising a third program, wherein the
2 second program authenticates to the third program by generating a third authentication
3 token from the first authentication token received from the first program, and sending the
4 third authentication token to the third program.

1 52. The program product of claim 51 wherein the third program verifies the third
2 authentication token by querying the public key authority for the public key
3 corresponding to the second program.

1 53. The program product of claim 41 further comprising log file that is written to each
2 time a program verifies an authentication token.

1 54. A program product comprising:
2 (A) an inter-program authentication mechanism that authenticates a first program
3 to a second program using a first authentication token that is digitally signed by the first
4 program using a key that is dynamically generated by a dynamic key generation
5 mechanism in a public key authority, the first program including an authentication
6 mechanism that authenticates a user; and
7 (B) computer-readable signal bearing media bearing the inter-program
8 authentication mechanism.

1 55. The program product of claim 54 wherein the computer-readable signal bearing
2 media comprises recordable media.

1 56. The program product of claim 54 wherein the computer-readable signal bearing
2 media comprises transmission media.

1 57. The program product of claim 54 wherein, after the inter-program authentication
2 mechanism authenticates the first program to the second program, the second program
3 performs identity mapping from an identity asserted by the first program to an identity
4 understood by the second program.

1 58. The program product of claim 54 wherein the first authentication token
2 comprises:
3 information about a user that authenticates with the first program;
4 information about the first program;
5 information about the second program; and
6 a digital signature of the first program using a private key for the first program
7 generated by the dynamic key generation mechanism.

1 59. The program product of claim 54 wherein the second program verifies the first
2 authentication token by querying the public key authority for the public key
3 corresponding to the first program.

1 60. The program product of claim 59 wherein the second program verifies the first
2 authentication token by verifying the digital signature of the first program using the
3 public key for the first program retrieved from the public key authority.

1 61. The program product of claim 54 wherein the second program authenticates to the
2 first program, if required, by digitally signing the first authentication token using a private
3 key corresponding to the second program to generate therefrom a second authentication
4 token, and returning the second authentication token to the first program.

1 62. The program product of claim 61 further comprising a third program, wherein the
2 second program authenticates to the third program by generating a third authentication
3 token from the first authentication token received from the first program, and sending the
4 third authentication token to the third program.

1 63. The program product of claim 61 wherein the third program verifies the third
2 authentication token by querying the public key authority for the public key
3 corresponding to the second program.

1 64. The program product of claim 54 further comprising a log file that is written to
2 each time a program verifies an authentication token.

1 65. A program product comprising:
2 (A) an inter-program authentication mechanism that authenticates a first program
3 to a second program using a first authentication token generated by the first program
4 using a public/private key pair corresponding to the first program, and that authenticates
5 the second program to a third program using a second authentication token that includes
6 all information in the first authentication token; and
7 (B) computer-readable signal bearing media bearing the inter-program
8 authentication mechanism.

1 66. The program product of claim 65 wherein the computer-readable signal bearing
2 media comprises recordable media.

1 67. The program product of claim 65 wherein the computer-readable signal bearing
2 media comprises transmission media.

* * * * *